INTERMEDIARY DEVICE INITIATED CALLER IDENTIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application is a divisional application and claims priority from U.S. Patent Application Serial No. 10/015,281 filed on December 12, 2001. The present application is also related to the following co-pending applications:

(1) U.S. Patent Application Serial No. 10/015,381 (Attorney Docket No. AUS920010818US1);

(2) U.S. Patent Application Serial No. 10/015,281 (Attorney Docket No. AUS920010819US1);

(3) U.S. Patent Application Serial No. 10/015,265 (Attorney Docket No. AUS920010820US1);

(4) U.S. Patent Application Serial No. 10/015,267 (Attorney Docket No. AUS920010821US1);

(5) U.S. Patent Application Serial No. 10/015,282 (Attorney Docket No. AUS920010822US1); and

(6) U.S. Patent Application Serial No. 10/015,280 (Attorney Docket No. AUS920010823US1).

(7) U.S. Patent Application Serial No. 10/022,160 (Attorney Docket No. AUS920010832US1).

(8) U.S. Patent Application Serial No. 10/022,158 (Attorney Docket No. AUS920010833US1).

(9) U.S. Patent Application Serial No. 10/022,161 (Attorney Docket No. AUS920010834US1).

(10) U.S. Patent Application Serial No. 10/022,624 (Attorney Docket No. AUS920010835US1).

(11) U.S. Patent Application Serial No. 10/022,164 (Attorney Docket No. AUS920010836US1).

(12) U.S. Patent Application Serial No. 10/022,163 (Attorney Docket No. AUS920010837US1).

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates in general to telecommunications and, in particular, to voice identification. Still more particularly, the present invention relates to initiating authentication of the identity of a caller at an intermediary device.

2. Description of the Related Art:

Telephone service has created communication channels worldwide, and those channels continue to expand with the advent of cellular and other wireless services. A person can simply take a telephone off-hook and dial a destination number or press a send button and be connected to a telephone line around the world.

Today, the public switching telephone network (PSTN), wireless networks, and private networks telephone services are based on the identification of the wireless telephone or wireline that a calling party uses. Services are personalized according to wireless telephone or wireline telephone number, where service associated with one telephone number are not accessible for another telephone number assigned to the same subscriber. For example, there is typically a first set of service features and billing options assigned to a home line number, a second set of service features and billing options assigned to an office line number, and a third set of service features and billing options assigned to a cellular telephone number. The networks process calls to and from each of these different subscriber telephones based on a separate telephone number.

A problem arises when a caller needs to access a service provided to one telephone number from another telephone number. Further, a problem arises when two or more people utilize a single line, but each want different sets of service options.

One of the services provided by many networks is caller identification. However, caller identification (caller ID) is limited to identification the wireline or wireless telephone number and the name of the subscriber of a service. Where multiple people share a single line, only the name of the person who establishes a service is displayed as the caller ID, often causing confusion about who is actually calling.

Therefore, in view of the foregoing, it would be advantageous to provide a method, system, and program for identifying an incoming call according to the identity of caller, rather than the number for the wireline or wireless service from which a call is made. In addition, it would be advantageous to provide a method, system, and program for specifying services available to a caller at any telephony device, rather than just those devices for which the caller is a subscriber.

Each service provided from by the PSTN must be extensively tested for faults and requires expensive hardware for implementation. Therefore, in view of the foregoing, it would be a further advantage to provide a method, system, and program for implementing services by devices external to the PSTN.

SUMMARY OF THE INVENTION

In view of the foregoing, it is therefore an object of the present invention to provide an improved telecommunications system.

It is another object of the present invention to provide a method, system and program for improved voice identification.

It is yet another object of the present invention to provide a method, system and program for initiating authentication of the identity of a caller at an intermediary device.

According to one aspect of the present invention, a caller places a call to a particular line number. The device receiving the call at the particular line number also preferably receives an authenticated identity of the caller placing the call.

According to another aspect of the present invention, a trusted telephone network detects a call initiation connection from an origin device. The trusted telephone network then brokers a connection between the origin device and an external server enabled to perform a caller identity authentication service. A voice utterance for a caller is received at the external server from the origin device. The server authenticates a caller identity associated with the voice utterance and transfer the authenticated caller identity to the trusted telephone network. The trusted telephone network then specifies services available for the call according to a caller profile for the authenticated caller identity.

All objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a block diagram of a network environment in which the present invention may be implemented;

Figure 2 illustrates a block diagram of the flow of a voice identifier authenticated by an intermediary device in accordance with the method, system, and program of the present invention;

Figure 3 depicts a block diagram of the flow of a voice identifier authenticated by an external system accessible from an intermediary device in accordance with the method, system, and program of the present invention;

Figure 4 illustrates a flow diagram of a signal flow and processing where an intermediary device authenticates a caller identity in accordance with the method, system, and program of the present invention; and

Figure 5 depicts a flow diagram of a signal flow and processing where an external system is accessed by an intermediary device to authenticate a caller identity in accordance with the method, system, and program of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A method, system, and program for intermediary device initiated caller authentication are provided. By authenticating a caller identity at an intermediary device, the caller identity may be transferred from the intermediary device to a destination device. The caller identity received at the destination device identifies the caller, rather than the line from which a call is made. An intermediary device may also utilize the authenticated caller identity to specify services available for a call, such that telephone lines are not limited to the services selected by the line subscriber.

One advantage of intermediary device caller identity authentication includes performing caller identification within a trusted network, wherein minimal security is necessary for transferring information within the trusted network. The intermediary device may include multiple telephone networks for multiple telephone service providers, where the service providers agree to a general level of trust for calls and information transferred across the telephone network boundaries.

However, performance of caller identity authentication within an intermediary device may be cost prohibitive in some cases because of the extensive software testing requirements and the cost of implementing hardware within the trusted network. Therefore, an intermediary device may initiate caller identity authentication by accessing an external system via an external network.

The external system includes a service that is advantageously able to authenticate the identity of a caller. Communications between the intermediary device and the external system may require an additional level of security and verification, since the external system is advantageously located outside the trusted network. Where an authenticated caller identity is utilized by an intermediary device to designate services available for a call, those services may also be accessible from an external system, accessible via an external network.

While in the present invention, authentication of a caller identity is described with emphasis placed on voice authentication, other methods of caller identity authentication may also be performed. Voice samples utilized for voice authentication are just one of multiple types of biometric sampling. For example, a caller may locally provide an eye scan, a fingerprint, and other biophysical identifiers that are transmitted within or outside the trusted network to authenticate the identity of the caller. Alternatively, keypad entries, such as a pin code, a credit card account number, password, or other secure transaction key may be entered by a caller and utilized to authenticate the identity of the caller.

In addition, while in the present invention, authentication of a caller identity is described with emphasis upon performing authentication at the beginning of a call, authentication of a caller identity may be performed continuously throughout a call, at selected points throughout a call, and after a call. Selected points where authentication may be performed include when an additional phone pick-up is detected, when a new voice is detected at the origin device, when a call is transferred from one telephone device to another, and other routing of a call that may result in a new caller or in a call being recorded.

Further, while the present invention is described with emphasis upon a caller identity authentication being made for a call to continue, a call may also continue without caller identity authentication. However, where a caller is not identifiable, it may be advantageous to automatically log that the caller lacks proper identification and automatically record calls that lack proper caller identification.

According to another advantage of the present invention, the identity of the device utilized by a caller may also be identified. First, the identity of the device may include the number from which a call is placed. In addition, the identity of the device may indicate the person to whom a device belongs. For example, a caller may call from a wireless business telephone.

For purposes of the present invention, telephony devices are termed origin devices when

utilized for origination of a call to an intermediary device and are termed destination devices when utilized for receipt of a call from an intermediary device. Subscribers to a call are termed callers when originating a call and are termed callees when receiving a call. Callers and callees may or may not be line subscribers to the particular line number utilized.

In the following description, for the purposes of explanation, numerous specific details are set forth to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form to avoid unnecessarily obscuring the present invention.

With reference now to the figures, and, in particular, with reference now to **Figure 1**, there is depicted a block diagram of a network environment in which the present invention may be implemented. While the present invention is described with reference to one type of network environment, it will be understood by one with skill in the art that the present invention may be implemented in alternate types of network environments.

GENERAL NETWORK ENVIRONMENT

First, the network environment incorporates a Public Switching Telephone Network (PSTN) **10**. As is known in the art the core of PSTN **10** may include multiple telephone networks, each owned by one of multiple independent service providers. Each telephone line is carried by an independent service provider within PSTN **10** and is typically assigned to at least one subscriber.

Switching of a call within an independent service provider=s telephone network is considered trusted movement within a trusted network because the call remains within the company=s telephone network infrastructure. However, calls may be transferred from one service provider=s telephone network to another service provider=s telephone network in generally trusted movement. Generally, service providers are in competition with one another

and therefore there is general trust in transferring a call, but not trust in sharing of subscriber information beyond a subscriber number and name from one service provider to the next without security features or other arrangements.

Advantageously, each telephone network within PSTN **10** may access a data network functioning as an extension to PSTN **10** via an Intranet. Data networks may include, for example, subscriber profiles, billing information, and preferences that are utilized by a service provider to specialize services. Transfer of information between a service provider=s data network and telephone network is trusted movement in sharing of information.

Further, each telephone network within PSTN **10** may access server systems external to PSTN **10** in the Internet Protocol over the Internet or an Intranet. Such external server systems may include an enterprise server, an Internet service provider (ISP), an access service provider (ASP), a personal computer, and other computing systems that are accessible via a network. In the present embodiment, transfer of information between PSTN **10** and server systems accessible via a network **20** is untrusted and therefore may require verification and additional security. Network **20** may be preferably considered an external network.

In the present invention, network **20** may comprise a private network, an Intranet, or a public Internet Protocol network. Specifically, telco application server **22**, generic application server **24**, pervasive application server **26**, and systems management server **28** represent server systems external to PSTN **10** that may be accessed by PSTN **10** over network **20**.

In particular, telco application server **22** preferably includes multiple telco specific service applications for providing services to calls transferred to a server external to PSTN **10**. In particular, a call may be transferred from PSTN **10** to telco application server **22** to receive at least one service and then the call is transferred back to PSTN **10**. PSTN 10 preferably brokers the connection between the telephony device and telco application server **22**. Such services may also be provided to calls within PSTN **10**, however placing such services at a third party such as telco application server **22,** is advantageous because adding services and information to PSTN **10**

is time consuming and costly when compared with the time and cost of adding the services through telco application server **22**.

In accord with an advantage of the present invention, as will be further described, the identity of both the caller and the callee may be authenticated by one of telephony devices **8a-8n**, PSTN **10**, or by telco application server **22**. By authenticating the actual identity of the person making a phone call and the person receiving the phone call, rather than the identification of a device from which a call is made and received, an enhanced specialization of services to subscribers may be performed.

An authentication service within telco application server **22** may include identification and verification of the identity of a caller and/or callee of a particular call. Such a service may require that subscribers provide voice samples when setting up a subscription. The stored voice samples may then be compared against voice samples received for a particular call in order to authenticate the identity of a current caller or callee of the particular call.

Generic application server **24** preferably accesses independent server systems that provide services. For example, a messaging server, a financial server, an Internal Revenue Service (IRS) server, and database management system (DBMS) server may be accessed in HTTP via network **20**. Each of these servers may include a telco service application that requires authentication of the subscriber before access is granted. For example, a financial server may provide a telco service application that allows an authenticated subscriber to access current financial records and request stock quotes from the financial server.

Pervasive application server **26** manages services for wirelessly networked devices. In particular, pervasive application server **26** preferably handles distribution of wireless packets of voice and data to wirelessly networked devices utilizing a standard such as short messaging service (SMS) messaging or other 3G standards.

Systems management server **28** manages subscriber personalization via the web. In particular, systems management server **28** includes browser technology that includes a provisioning console **30** for establishing a subscriber profile and a management console **32** for managing and updating the subscriber profile. A subscriber preferably accesses the consoles of systems management server **28** via the Internet utilizing a computing system, such as computing systems **34a-34n**.

The subscriber profile may be accessed at systems management server **28** by other external servers and PSTN **10** via network **20**. In addition, a local copy of a subscriber profile updated in systems management server **28** may be stored within a particular service provider=s data network or telephone network. Each service provider may specify the types of preferences and other information included within a subscriber profile.

In particular, a subscriber may provide a voice imprint when establishing a subscriber profile through provisioning console **30**. Other types of authentication information may also be provided including, but not limited to, a password, an eye scan, a smart card ID, and other security devices. In addition, a subscriber may designate billing preferences, shopping preferences, buddy list preferences, and other preferences that enable specialized service to the subscriber when the subscriber=s identity is authenticated from the voice imprint or other identification.

Advantageously, a management agent is built into each external server to monitor the services provided by each server according to the authenticated subscriber receiving the services. By monitoring service output according to subscriber, the subscriber may then be billed according to each use of a service.

PSTN **10** preferably includes both voice and data signaling networks that interface with network **20** via gateways. Each of the gateways acts as a switch between PSTN **10** and network **20** that may compress a signal, convert the signal into Internet Protocol (other protocol) packets, and route the packets through network **20** to the appropriate server.

In particular, the voice network interfaces with network **20** through media gateway **14** which supports multiple protocol gateways including, but not limited to, SIP. SIP is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.

In addition, in particular, the data signaling network interfaces with network **20** through signaling gateway **12** which supports multiple protocol gateways including, but not limited to, parlay protocol gateways and SS7 protocol gateways. Internet servers, such as telco application server **22** may include protocol agents that are enabled to interact with multiple protocols encapsulated in Internet Protocol packets including, but not limited to, SS7 protocol, parlay protocol, and SIP.

IDENTITY AUTHENTICATION AND CALL CONTROL

Looking into PSTN **10**, a telephone network typically includes multiple switches, such as central office switches **11a-11n**, that originate, terminate, or tandem calls. Central office switches **11a-11n** utilize voice trunks for transferring voice communications and signaling links for transferring signals between signaling points.

Between signaling points, one central office switch sends signaling messages to other central office switches via signaling links to setup, manage, and release voice circuits required to complete a call. In addition, between signaling points, central office switches **11a-11n** query service control points (SCPs) **15** to determine how to route a call. SCPs **15** send a response to the originating central office switch containing the routing number(s) associated with the dialed number.

SCPs **15** may be general purpose computers storing databases of call processing information. While in the present embodiment SCPs **15** are depicted locally within PSTN **10**, in alternate embodiments SCPs **15** may be part of an extended network accessible to PSTN **10** via a

network.

One of the functions performed by SCPs **15** is processing calls to and from various subscribers. For example, an SCP may store a record of the services purchased by a subscriber, such as a privacy service. When a call is made to the subscriber, the SCP provides record of the privacy service to initiate an announcement to a caller to identify themself to the subscriber with the privacy service who is being called. According to an advantage of the invention, authentication of the subscriber receiving the call may be required before the privacy service is initiated for that subscriber.

In particular, network traffic between signaling points may be routed via a packet switch called an service transfer point (STP) **13**. STP **13** routes each incoming message to an outgoing signaling link based on routing information. Further, in particular, the signaling network may utilize an SS7 network implementing SS7 protocol.

Central office switches **11a-11n** may also send voice and signaling messages to intelligent peripherals (IP) **17** via voice trunks and signaling channels. IP **17** provides enhanced announcements, enhanced digit collection, and enhanced speech recognition capabilities.

According to an advantage of the present invention, the identity of a caller is authenticated according to voice authentication. Voice authentication is preferably performed by first identifying a subscriber by matching the name or other identifier spoken with a subscriber name or identifier. Next, voice authentication requires verifying that the voice audio signal matches that of the identified subscriber. However, in alternate embodiments, the identity of a subscriber may be authenticated according to passwords, eye scans, encryption, and other security devices.

In particular, to perform subscriber authentication of audio signals received from callers, IP **17** may include storage for subscriber specific templates or voice feature information, for use in authenticating subscribers based on speech. If a subscriber specific template is not stored on a

local IP **17**, then a remote IP containing the subscriber specific template may be accessed via a network. In addition, local IP **17** may access systems management server **28** or another repository for voice imprints to access the subscriber specific template.

Where IP **17** authenticates the identity of a caller (e.g. the subscriber placing a call), a voice identifier (VID) representing the authenticated caller identity is transferred as a signal for identifying the caller. In addition, where IP **17** authenticates the identity of a callee (e.g. the subscriber receiving a call), a reverse VID (RVID) including the callee identity is transferred as a signal for identifying the callee.

Alternatively, to perform subscriber authentication of audio signals received from callers, PSTN **10** may broker a caller identity authentication service from telco application server **22**. In particular, a signaling channel is opened between central office switches **11a-11n** and telco application server **22** via signaling gateway **12**. In addition, a voice channel is opened between central office switches **11a-11n** and telco application server **22** via media gateway **14**.

Because telco application server **22** is located outside of the trusted network, there may be a time delay associated with establishing a connection to telco application server **22** and authenticating the identity of a caller that is longer than a time delay present where a caller identity is authenticated by IP **17**. However, offloading services outside the trusted network allows greater creativity and competition in providing telephone services.

In addition, because telco application server **22** is located outside of the trusted network, it is advantageous to establish a level of security for transactions between telco application server **22** and central office switches **11a-11n**, wherein the level of security is suitable for untrusted communications. A level of security may be implemented by by utilizing security based protocols, such as the secure socket layer, and by applying ordinary encryption. In particular, the level of security preferably protects the communication channel between telco application server and PSTN **10** and authenticates the identity of the server from which a caller identity authentication service is accessed. Therefore an additional feature of signaling gateway **12** and

media gateway **14** is security verification.

Advantageously, VIDs indicate through text, voice, or video the identity of a caller. For example, a caller=s name may be transferred as the identity of a caller. Alternatively, a video clip stored with the subscriber template may be transferred as the identity of a caller. Additionally, VIDs may indicate the identity of the device utilized by a caller to provide context for a call. Further, VIDs may indicate which system or systems have authenticated the caller identity.

After a VID and/or RVID are determined by IP **17**, IP **17** and SCP **15** may communicate to designate which services are available according to VID and RVID. Advantageously, by designating services according to a VID and/or RVID, subscribers are provided with services and billed for those services independent of the devices utilized by subscribers. In particular, a 1129 protocol or other protocol may be utilized to enable signal communications between IP **17** and SCPs **15**.

In addition, as previously described, caller authentication to determine VIDs and RVIDs may be performed by an external system, such as telco application server **22**. The VID or RVID returned from telco application server **22** may be transferred from central office switches **11a-11n** to SCP **15** in order to access a subscriber profile associated with the VID or RVID. Alternatively, the VID or RVID may first transfer to IP **17**, where additional verification of the caller identity is performed. For example, IP **17** may control distribution of the VID to the caller, where the caller is prompted to enter a password or additional information. IP **17** may then initiate loading the caller profile into central office switches **11a-11n** if the additional caller input is verifiable for the VID.

An origin telephony device or destination telephony device may also determine a VID and/or RVID for the caller and/or callee of a call. In particular, telephony devices **8a-8n** and call centers **16a-16n** may function as origin and destination telephony devices. Each of the telephony devices may include a database of voice templates that may be matched to authenticate the

identity of a caller or callee. In addition, each of the telephony devices may access a third party, such as telco application server **22**, to authenticate the identity of the caller or callee. In either case, the telephony device transmits a VID and/or RVID with a call to PSTN **10**.

Telephony devices **8a-8n** may include, but are not limited to wireline devices, wireless devices, pervasive device equipped with telephony features, a network computer, a facsimile, a modem, and other devices enabled for network communication. Advantageously, as previously described, a voice authentication functioning device may be included in each of telephony devices **8a-8n**.

In addition, telephony devices **8a-8n** may each incorporate a display that provides a visual output of a VID or RVID. Alternatively, such a display may be provided in a separate device connected to the line in parallel to telephones **8a-8n**. According to one advantage of the present invention, the identity of the actual caller or actual callee are output to a display in association with a call. In addition, other context information about the caller including, but not limited to, the device from which the call originates or is answered, ratings for a caller or callee, and other context information may be output to a display in association with a call.

Telephony devices **8a-8n** are communicatively connected to PSTN **10** via wireline, wireless, ISDN, and other communication links. Preferably, connections to telephony devices **8a-8n** provide digital transport for two-way voice grade type telephone communications and a channel transporting signaling data messages in both directions between telephony devices **8a-8n** and PSTN **10**.

In addition to telephony devices **8a-8n**, advanced telephone systems, such as call centers **16a-16n**, may be communicatively connected to PSTN **10** via wireline, wireless, ISDN and other communication links. Call centers **16a-16n** may include PBX systems, hold queue systems, private network systems, and other systems that are implemented to handle distribution of calls to multiple representatives or agents.

Returning to central office switches **11a-11n**, typically, one central office switch exists for each exchange or area served by the NXX digits of an NXX-XXXX (seven digit) telephone number or the three digits following the area code digits (NPA) in a ten-digit telephone number. The service provider owning a central office switch also assigns a telephone number to each line connected to each of central office switches **11a-11n**. The assigned telephone number includes the area code (NPA) and exchange code (NXX) for the serving central office and four unique digits (XXXX).

Central office switches **11a-11n** utilize office equipment (OE) numbers to identify specific equipment, such as physical links or circuit connections. For example, a subscriber=s line might terminate on a pair of terminals on the main distribution frame of one of central office switches **11a-11n**. The switch identifies the terminals, and therefore a particular line, by an OE number assigned to that terminal pair. For a variety of reasons, a service provider may assign different telephone numbers to the one line at the same or different times. For example, a local carrier may change the telephone number because a subscriber sells a house and a new subscriber moves in and receives a new number. However, the OE number for the terminals and thus the line itself remains the same.

On a normal call, a central office switch will detect an off-hook condition on a line and provide a dial tone. The switch identifies the line by the OE number. The central office switch retrieves profile information corresponding to the OE number and off-hook line. Then, the central office switch receives the dialed digits from the off-hook line terminal and routes the call. The central office switch may route the call over trunks and possibly through one or more central office switches to the central office switch that serves the called party=s station or line. The switch terminating a call to a destination will also utilize profile information relating to the destination, for example to forward the call if appropriate, to apply distinctive ringing, etc.

In the present invention, when a central office switch detects an off-hook condition on a line, the central office switch will then determine if a VID signal is transferred from the off-hook telephony device. If a VID is transferred, then a query is made to SCP **15** according to the VID

for any services specified for the authenticated subscriber. Alternatively, a query may be transferred via network **20** to an external server, such as system management server **28**, to determine the services specified for the caller. The central office switch will then receive the dialed digits from the off-hook line terminal and route the call, providing services according to those preferred by the authenticated subscriber.

In addition, an RVID may be provided in the present invention to authenticate the identity of a callee receiving the call. When a call is answered, the call is transferred back to an IP or telco application server **22** to authenticate the identity of the callee answering the call.

Further, a call may be forwarded or transferred to another line number. Preferably, for each caller identified, the line number and VID are determined and stored for the call, such that a callee is able to view the path of a call. In particular, the path preferably designates both the callers accessed and the line numbers accessed. In a three-way call, conference call, or other multi-party communication, tracing the path of VIDs, RVIDs, and line numbers for a call and presenting that path to current parties is advantageous.

As another alternative to dialed digits from the off-hook line terminal, a caller may utilize a voice calling function of a telephony device for indicating how the call should be routed. For example, a caller may say the name of a preferred callee. The device or IP **17** may determine a person within the caller=s calling list that matches the voiced name. The matching person=s digits are then utilized to route the call.

VID AUTHENTICATION CONTEXT

Referring now to **Figure 2**, there is illustrated a block diagram of the flow of a voice identifier authenticated by an intermediary device in accordance with the method, system, and program of the present invention.

As depicted, an intermediary device **42** authenticates a VID for a current caller.

Intermediary device **42** may include a PSTN switching network or networks. However, intermediary device **42** may also include a PBX, a call center, or other private switching system. Further, intermediary device **42** may include network servers, telco application servers, Websphere7 (Websphere7 is a registered trademark of International Business Machines, Inc.) servers, and other systems which provide call processing.

An origin device **40** is utilized by a caller to initiate a call. A caller may provide a voice utterance which is transferred from origin device **40** to intermediary device **42** for purposes of caller identity authentication. Intermediary device **42** may include at least one IP with access to an extended database of voice samples, combined into a service identification/verification (SIV) function **45**. SIV function **45** compares the voice utterance with the voice samples to authenticate the identity of a caller as a VID. Then, intermediary device **42** may access a caller profile and other contextual information about a caller according to the VID. In addition, SIV function **45** may continue to monitor the caller voice continuously during a call and at selected points throughout the call. In particular, if another telephone device on the same line number as origin device **40** is detected off-hook, caller identity authentication may be triggered.

Intermediary device **42** connects origin device **40** with a destination device **44**. In particular, destination device **44** may include a callee telephony device, as previously described. However, destination device **44** may also include a PBX, call center, or other private switching system that manages multiple telephony devices. Moreover, destination device **44** may include network servers, feature servers, client side devices, and other systems which provide call receipt.

The authenticated VID may be filtered and distributed to multiple locations. In particular, the VID may be recorded for the call. Then, the VID is preferably filtered according to caller preferences, callee preferences, and intermediary device preferences. In particular, a caller profile may include a request to block a VID from transfer to a callee. Alternatively, a caller profile may include different titles, names, and other identifiers that are filterable according to the callee RVID. For example, if the callee is a business associate, then the VID may be filtered to

include the caller=s full name and position. However, if the callee is a friend, then the VID may be filtered to include the caller=s nickname. Filtering and blocking may be performed by a filtering service within trusted telephone network **46** and/or outside trusted telephone network **46**. A caller may also block the VID from being distributed to online vendors and others with access to VIDs and RVIDs of current calls.

When not blocked by the caller, the authenticated VID is preferably transferred from intermediary device **42** to destination device **44** with a call. Destination device **44** advantageously includes a display device or other output interface for output of the authenticated VID to the callee, such that the identity of the caller of an incoming call is provided to the callee.

An advantage of the present invention is that the caller of a call may be identified without identifying the caller=s phone number to be captured by a recipient. However, in some cases it may be advantageous that the VID also include other information that provides a context for a call. For example, the intermediary device **42** preferably captures and stores the line number utilized to place a call. In a setting where a representative of a business calls a customer and the representative if unable to answer the customer=s question, the representative may transfer the customer to another caller/representative. Monitoring both the VID and the extension or line number of the new representative is advantageous. Other settings in which including a line number of a new caller within a VID are understood to be incorporated.

Other examples of context information include, but are not limited to, the GPS location or time zone of the caller location, the device from which the call is placed, the subject matter of the call, and whether the caller is calling on behalf of another, may be included in a VID. Further, the identity of the device that performed the caller authentication may be included in a VID.

A VID may be transferred in multiple protocols, including, but not limited to, Interface Definition Language (IDL). A VID may include a range of information, where each type of information may be tagged or identified in some other manner. For example, the following

tagged VID may be transmitted to represent an authenticated identity of a caller:

[name] Jon Smith
[device] Jane Doe=s cell phone
[location] Central Time zone
[subject] Project A
[authenticated by] External authentication service #40

With reference now to **Figure 3**, there is depicted a block diagram of the flow of a voice identifier authenticated by an external device accessible from an intermediary device in accordance with the method, system, and program of the present invention.

As illustrated, intermediary device **42** may access an external system with a request for caller identity authentication. In the present embodiment, intermediary device **42** connects to external network **20** via signal and media gateways. In particular, by accessing services via external network **20**, intermediary device **42** reaches outside of trusted network boundary **46**. Therefore, additional levels of security, such as transfer of information utilizing a secure socket layer (SSL) and authenticating the location of a server performing the services, may be required.

Telco application server **22** provides an external system enabled to authenticate a caller identity. Telco application server **22** may include an application that functions to identify a voice utterance and verify the voice utterance by comparison with a voice sample. Telco application server **22** may access external databases of voice samples. In addition, telco application server **22** may access voice samples via a general applications server, a systems management server, or telephony devices accessible via network **20**.

Telco applications server authenticates a caller identity as a VID that is transferred into trusted network boundary **46** to reach intermediary device **42**. Intermediary device **42** may then transfer the VID to destination device **44**. In addition, intermediary device **42** may utilize the VID to access a caller profile within the trusted network or from an external system. In

particular, a complete caller profile may be combined from accessing caller profile components from systems within the trusted network and external to the trusted network.

Another function of telco application server **22** is providing voice samples from a database to intermediary device **42**. Intermediary device **42** may then perform caller identity authentication utilizing the voice samples received from telco application server **22**. Telco application server **22** may access voice samples from multiple data storage systems accessible via network **20**.

By accessing a VID or voice samples from telco application server **22**, the functionality of intermediary device **42** is expanded without requiring the addition of costly hardware to intermediary device **42**. Extending outside trusted network boundary **46** to transfer a call or access information may require additional layers of security and verification, however moving services outside trusted network boundary **46** will allow an increase in services and greater competition to provide services.

Further, telco application server **22** may continue to monitor a call while the call is in progress. A periodic sampling may be taken of a caller voice. In addition, triggers, such as detecting another phone off-hook for the caller line number, may initiate sampling current caller voices.

Referring now to **Figure 4**, there is illustrated a flow diagram of a signal flow and processing where an intermediary device authenticates a caller identity in accordance with the method, system, and program of the present invention. A standard telephone device is assumed for the Atel@ origin device in the present example. However, a similar signal flow may be applied to other types of origin devices.

The caller lifts a handset creating an off-hook state in the origin device and a corresponding change in state of an off-hook signal to the central office (step S1). In response to detecting an off-hook signal at the central office, a dial tone may be extended to the origin device

(step S2). Alternatively the dial-tone may be extended to the origin device after a caller profile has been loaded. In addition, when an off-hook signal is detected at the central office, a register is preferably assigned to the call.

In response to detecting an off-hook state, the central office also triggers a SIV initiation to an IP within the PSTN network (step S3). The call is preferably transferred to the IP such that a voice channel and signal channel are opened between the origin device and the IP. The IP preferably responds to a SIV initiation with a prompting instruction to the caller to provide specific identifying information (step S4). It should be mentioned that although the IP could passively monitor any speech that the caller may utter, it is advantageous to specifically prompt the caller. For example, the IP may play an audio prompt message asking the caller to APlease say your full name.@ In addition, the prompt may request other identifying information such as a service provider and subject of the call, for example. Further, the central office may trigger a SIV initiation to an IP at other times during a call. The spoken identification information at the origin device is transferred from the central office back to the IP (step S5).

Analysis is performed on the spoken identification information to determine a name of a caller and extract speech characteristics information (step S6). A voice template or other voice pattern information may be stored at a data storage system within an extended network accessible within the trusted network boundary according to a caller identity. In addition, as will be described in **Figure 5**, a voice template or other voice pattern information may be stored at an external data storage system accessible outside the trusted network boundary according to a caller identity.

Preferably, the SIV function of an IP compares the extracted speech information to the stored pattern information, to identify and authenticate the particular caller. If there is a match between the extracted speech information and the stored pattern information, then a VID signal containing the authenticated identity of the caller is transferred to the central office for storage in the register assigned to the call (step S7). In addition, the call is returned with the VID to the central office and the VID is stored in the SCP.

In addition to authenticating the identity of the caller placing a call, the identity of the device utilized to place the call and the line number utilized to place the call may be included in a VID. Each origin device may include an identification number that is stored in the register assigned to a call and attached to the VID of a call by the central office. Alternatively, where a single OE line includes multiple outlets, the device at each outlet may be identified according to the location of the outlet. Moreover, the context of a call, including a device identity, may be inferred from the location of the device, the line number of the device, and other context information.

Once a VID is received at the central office for a call, the central office triggers a request to an SCP for a caller profile according to the VID (step S9). The SCP searches for a caller profile in a local data storage system or a remote data storage system within the extended trusted network. Alternatively, the SCP may access the caller profile according to VID from a data storage system accessible outside the trusted network boundary. Further, in lieu of, or in addition to the information stored at the SCP, a request may be extended from the PSTN to other servers storing information about a caller according to caller profile, depending on the services to be provided to a caller. The SCP returns a caller profile that indicates additional personal information about a caller, billing information, and services selected by a caller (step S10). The central office loads the profile into the register associated to the call (step S11). Next, dialed digits may be received from the origin device (step S12). Alternatively, dialed digits may be received at any point after a dial tone is provided, where the dialed digits are stored in the register for a call until the caller profile is loaded.

Next, the VID is filtered (step S13). The VID may be filtered to block the VID from transfer to the callee, to specify content of the VID for transfer to the callee, and to specify the content of the VID for access by a data mining service or online retailers.

The call is then processed for the dialed digits according to the caller profile (step S14). The, the VID is transferred via the signal channel to the destination device (step S15). The

destination device preferably controls output of the VID via, for example, a graphical user interface or a speaker, such that a callee is enabled to decide whether to answer to a call from an identifier caller.

The importance of forwarding the caller VID to the destination device is that the callee receives the identity of the caller, not just the line number from which the call is received. Output of a caller VID, including a caller name, device identification, geographic context, and other information, is more advantageous than a typical caller ID that indicates the line number and person billed for the line number because with the VID, the actual caller is identified, but the actual line number may be blocked from the callee or displayed to the callee. In particular, blocking a line number may be advantageous where a caller does not want the callee to be able to capture the line number.

If there is not a match of the extracted speech information with the voice templates, then a determination is made as to whether a caller has made more than n tries to speak identification information that has not matched (step S8). If the caller has not made more than n tries, then a prompt is output to the caller to provide another spoken utterance. If the caller has made more than n tries, then a denial signal is transferred to the central office (step S16). In addition, instructions for creating a voice template may be provided or an off-hook signal or change in state of the line without an associated VID may be sent from the central office, such that the caller is enabled to place a call utilizing the services associated with the OE of the line. In addition, the central office may automatically initiate recording of the call where a caller identity is not authenticated.

It should be noted that with each transfer of an VID, the central office, the SCP, and the destination device may each record and filter the VID. In particular, filtering the VID may require blocking all or portions of the content of the VID.

With reference now to **Figure 5**, there is depicted a flow diagram of a signal flow and processing where an external system is accessed by an intermediary device to authenticate a

caller identity in accordance with the method, system, and program of the present invention.

In response to receiving on off-hook state at the central office, a register is created for a call. A request for a caller authentication service is initiated by the central office to the signaling and media gateways (step S20). The signaling gateway initiates a secure signal channel between the central office and a telco application server that provides a caller authentication service (step S21). The media gateway initiates a secure media channel between the central office and the telco application server (step S22). Further, the central office may trigger a caller authentication service at other times during a call.

The call may then be transferred to the telco application server, however the central office brokers the communication channels between the telco application server and origin and destination devices. In particular, the telco application server may allow a callee to listen to the caller identity authentication process or parts of the process. Alternatively, only a connection between the telco application server and the origin device may be brokered.

To provide service, the authorization service application of the telco application server provides a prompting instruction to the caller to provide specific identifying information (step S23). For example, the authorization service application may play an audio prompt message asking the caller to APlease say your full name.@ In addition, the prompt may request other identifying information such as a service provider and subject of the call, for example. The spoken identification information is then received at the central office from the origin device and transferred via the media gateway to the telco application server (step S24).

Analysis is performed on the spoken identification information to determine a name of a caller and extract speech characteristics information (step S25). A voice template or other voice pattern information may be accessible to the telco application server from a local or remote database management system. Preferably, the authorization service application compares the extracted speech information to the stored pattern information, to identify and authenticate the particular caller. If there is a match between the extracted speech information and the stored

pattern information, then a VID signal containing the authenticated identity of the caller is then distributable to the central office (step S26) and the call is returned to the central office.

If there is not a match of the extracted speech information with the voice templates, then a determination is made as to whether a caller has made more than n tries to speak identification information that has not matched (step S27). If the caller has not made more than n tries, then a prompt is output to the caller to provide another spoken utterance. If the caller has made more than n tries, then a denial message is output to the central office (step S28). In addition, instructions for creating a voice template may be provided.

It should be noted that with each transfer of an VID, the central office, signaling gateway, telco application server, and destination device may each record and filter the VID. In particular, filtering the VID may require blocking all or portions of the content of the VID.

It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media, such as a floppy disk, a hard disk drive, a RAM, CD-ROMs, DVD-ROMs, and transmission-type media, such as digital and analog communications links, wired or wireless communications links using transmission forms, such as, for example, radio frequency and light wave transmissions. The computer readable media may take the form of coded formats that are decoded for actual use in a particular data processing system.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.